In the Claims:

Please cancel claims 1-4, 8-9, and 13-18. Please amend claims 5-7 and 10-12. Please add new claims 19-30. The claims are as follows:

1-4. (Canceled)

5. (Currently amended) A method of operating an intrusion detection system, comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service attack attempting to impede operation of the protected device; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

when the value of the signature event counter exceeds the signature threshold quantity, generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of an the intrusion detection system to decrease an alert generation rate of an the intrusion detection sensor.

6. (Currently amended) The method of claim 5, wherein the element is [[a]] the signature threshold quantity.

7. (Currently amended) The method of claim 5, wherein the element is a signature threshold interval that specifies a sliding time window.

8-9. (Canceled)

10. (Currently amended) Programmable media containing programmable software for operation of an intrusion detection system, programmable software comprising the steps of:

monitoring, by the intrusion detection system, for occurrence of a signature event that is indicative of a denial of service intrusion on a protected device, said denial of service attack attempting to impede operation of the protected device; and

when a signature event occurs, increasing a value of a signature event counter and comparing the value of the signature event counter with a signature threshold quantity; and

when the value of the signature event counter exceeds the signature threshold quantity, generating an alert by an intrusion detection sensor of the intrusion detection system, recording a time of generating the alert in a log of a governor comprised by the intrusion detection sensor, determining from contents of the log a present alert generation rate, and comparing the present alert generation rate with an alert generation rate threshold; and

when the present alert generation rate exceeds the alert generation rate threshold, altering an element of a signature set of ~~an~~ the intrusion detection system to decrease an alert generation rate of ~~an~~ the intrusion detection server.

11. (Currently amended) The programmable media of claim 10, wherein the element is [[a]] the signature threshold quantity.

12. (Currently amended) The programmable media of claim 10, wherein the element is a signature threshold interval that specifies a sliding time window.

13-18. (Canceled)

19. (New) The method of claim 5, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protect device.

20. (New) The method of claim 5, wherein the alert generation rate threshold is comprised by the governor.

21. (New) The method of claim 5, wherein the signature set comprises a unique signature set identifier, the signature event, the signature event counter, the signature threshold quantity, and a signature threshold interval that specifies a sliding time window.

22. (New) The method of claim 5, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

23. (New) The method of claim 5, wherein the method further comprises the step of entering into the log a list of timestamps that record the times at which the intrusion detection sensor generates alerts, wherein said determining from contents of the log a present alert generation rate utilizes the timestamps in the log.

24. (New) The method of claim 5, wherein after generating the alert and before determining from contents of the log the present alert generation rate, the method further comprises the step of:

clearing the log of any entries that are past a specified age.

25. (New) The programmable media of claim 10, wherein said generating the alert comprises alerting an administrator of suspected denial of service intrusions upon the protect device.

26. (New) The programmable media of claim 10, wherein the alert generation rate threshold is comprised by the governor.

27. (New) The programmable media of claim 10, wherein the signature set comprises a unique signature set identifier, the signature event, the signature event counter, the signature threshold

quantity, and a signature threshold interval that specifies a sliding time window.

28. (New) The programmable media of claim 10, wherein the protected device is selected from the group consisting of a computer, a web server, and a workstation.

29. (New) The programmable media of claim 10, wherein the programmable software further comprises the step of entering into the log a list of timestamps that record the times at which the intrusion detection sensor generates alerts, wherein said determining from contents of the log a present alert generation rate utilizes the timestamps in the log.

30. (New) The programmable media of claim 10, wherein after generating the alert and before determining from contents of the log the present alert generation rate, the programmable software further comprises the step of:

clearing the log of any entries that are past a specified age.